Audit Report
Emergency Command Centers

Prepared by:
CAL FIRE Office of Program Accountability

August 2010

Preface

In August 2009, the California Department of Forestry and Fire Protection (CAL FIRE) Office of Program Accountability (OPA) began an internal audit of the Department's Emergency Command Centers (ECC).

As part of its annual risk assessment and review of internal controls, OPA identified the Computer Aided Dispatch (CAD) system refresh in June of 2009, as a vital component in meeting CAL FIRE's mission. As such, OPA conducted an audit to verify and validate the system's operations for CAL FIRE management. In addition, OPA audited individual units for adherence to published CAL FIRE policy and procedures, Department of General Services' 9-1-1 Standards, and California Government Code §53100-§53120.

We appreciate the cooperation extended by the staff of CAL FIRE's 21 Units and both Regional Offices, and we thank them for their completion of the initial survey as well as their patience, cooperation, and honesty throughout the entire process.

This report communicates the results of our review.

STAFF:

Anthony P. Favro, Chief of Program Accountability
Rod Breitmaier, Auditor
George Alves, Auditor
Tajinder Bassi, Auditor

Table of Contents

Preface i

Table of Contents ii

Auditor's Report 1

Summary 2

Background 3

Scope, Methodology, and Objectives 4

Conclusion 5

Findings and Recommendations 6

Finding #1 – Server Rooms Inadequately Secured 6

Finding #2 – Inadequate Server Room Circulation 8

Finding #3 – Active Sprinkler Systems 10

Finding #4 – Lack of Temperature Alarm Sensor 12

Finding #5 – Crawlspace Access 14

Finding #6 – Command Center Access 15

Finding #7 – Expanded Command Center Access 16

Finding #8 – Disaster Recovery Plan Location 18

Finding #9 – Outdated Disaster Recovery Plan 20

Auditor's Report

Del Walters, Director
Department of Forestry and Fire Protection
1416 Ninth Street, Suite 1505
Sacramento, California 95814

The Office of Program Accountability (OPA) has completed its operational audit of the CAL FIRE Emergency Command Centers (ECC) located in the two regions and 21 units managed by the California Department of Forestry and Fire Protection (CAL FIRE).

The audit was conducted in accordance with *The International Professional Practices Framework,* issued by the Institute of Internal Auditors; additionally OPA utilized State Government Code, Department of General Services 9-1-1 Standards, and CAL FIRE's published policies and procedures governing ECCs that are contained in the Department's *Command and Control Handbook (8100)*. OPA also used the Department's *0900 Information Technology Services Handbook (0900)* for access control measurement.

OPA staff performed this review to ensure that the aforementioned CAL FIRE policies and procedures were followed during the period of review and that State assets were utilized in a manner consistent with State and CAL FIRE laws, rules, and regulations. To complete this audit, OPA staff distributed surveys to both regions and all 21 units and conducted on-site audit reviews of 13 ECCs, interviewing key staff and management. During the survey review and subsequent visits, OPA staff reviewed controls over physical security, access, operations, disaster recovery, and training.

Overall, the ECCs are operating effectively and efficiently. However, our review has indicated instances of non-compliance with CAL FIRE policy, as well as weaknesses in internal controls, physical security, access control, operations, and disaster recovery.

Enclosed is the Final Report for this review, including program responses. This report is intended for the information of the CAL FIRE Director, CAL FIRE management, and its designees and is not intended to be used by anyone other than the designated parties.

Anthony P. Favro

Anthony P. Favro
Chief of Program Accountability

August 16, 2010

Summary

In 2009/10, the California Department of Forestry and Fire Protection (CAL FIRE) Office of Program Accountability (OPA) conducted an audit of the Emergency Command Centers (ECCs) managed by CAL FIRE.

The audit was conducted to determine that established policies, procedures, and standards exist and are employed for physical security, access control, operations, disaster recovery, and training. Additionally, OPA sought to verify that the Computer Aided Dispatch (CAD) refresh project implemented in June 2009 is operating efficiently and effectively.

OPA has verified that internal controls are generally operating as designed and implemented for the ECCs, with some exceptions, which are detailed in the Findings and Recommendations section of this report.

Background

CAL FIRE's firefighters, fire engines, and aircraft respond to over 5,600 wildland fires and answer the call more than 350,000 times for other emergencies each year. The Department is responsible for protecting over 31 million acres of California's privately owned wildlands and for emergency services of all varieties in 35 of California's 58 counties through contracts with local governments.

CAL FIRE's ECCs are the backbone of the Department's emergency response mission. Located in each of CAL FIRE's two regions and 21 administrative units statewide, the ECCs are responsible for dispatching CAL FIRE resources to emergency incidents within their operational area and for coordinating the movement of resources to ensure that the Department is able to fulfill its critical mission.

Direction for assurance of effective and efficient operations in CAL FIRE's ECCs is outlined by the Department's policy and procedures handbooks. CAL FIRE *Information Technology Services Handbook (0900)* outlines internal controls for physical security and access control to CAL FIRE Information Technology (IT) assets, while the *Command and Control Handbook (8100)* describes operational requirements for staffing levels and fire response plans. The *Command and Control Handbook* also provides direction for disaster recovery processes, training requirements of ECC staff, and serves as CAL FIRE's operational manual for ECCs.

When this audit project was initiated, the Department of General Services (DGS) maintained the California State 9-1-1 Emergency phone services program. For compliance purposes, OPA used DGS's *State of California 9-1-1 Operations Manual CHAPTER I – STANDARDS* (Revised November 2008). The 9-1-1 program is now under the direction of the State Chief Information Office (OCIO); however, there have been no published reports of the 9-1-1 standard being modified or revised as of this report date.

In addition, OPA used California Government Code §53100-§53120, also known as the Warren-911-Emergency Assistance Act, for compliance.

The CAL FIRE Handbooks, OCIO 9-1-1 Standard, and California Government Code establish standards, policy, and procedures that ensure that:

- CAL FIRE resources are guarded against improper procurement, use, and allocation.
- CAL FIRE ECCs operate in an efficient and effective manner.
- Weaknesses in CAL FIRE internal controls are easily detected, identified, and mitigated in a timely manner.
- CAL FIRE resources are protected both physically and logically.
- CAL FIRE resources, both staff and IT, are utilized in an efficient and effective manner.

Scope, Methodology, and Objectives

This audit covered ECC operations from June 2009 through May 2010. The refresh of the CAD system necessitated a review of acceptability by end users. The CAD is an essential resource used by CAL FIRE to fulfill its critical resource protection and emergency response mission. As such, verification and validation of end user acceptability is paramount.

In September 2009, OPA distributed a survey to ECCs in the two regions and all 21 units and requested the return of completed surveys by November 2009. Upon receipt, OPA staff reviewed each of the surveys and noted any deficiencies identified. OPA staff then conducted an informal risk assessment on the completed surveys and selected ECCs for on-site visits for further validation. OPA selected 13 of 21 ECCs for on-site visits and worked through local ECC management to conduct the visits, including entrance and exit conferences, observations, and interviews with key personal. The auditors noted deficiencies in internal controls, physical security, access control, operations, and disaster recovery; relayed their findings to ECC management; and included these findings in this report.

OPA staff verified and validated that:

- CAL FIRE resources are guarded against improper procurement, use, and allocation.
- CAL FIRE ECCs operate in an efficient and effective manner.
- Weaknesses in CAL FIRE internal controls are easily detected, identified, and mitigated in a timely manner.
- CAL FIRE resources are protected both physically and logically.
- CAL FIRE resources, both staff and IT, are utilized in an efficient and effective manner.

Conclusion

The internal controls employed by CAL FIRE management for the operation of its ECCs are functioning as intended, except where noted in this report in the Findings and Recommendations section. Overall, CAL FIRE's ECCs are very efficient and effective operations that provide services 24 hours a day, 7 days a week without significant interruption or loss of communications that might cause great harm or damage.

OPA recommends that CAL FIRE's Fire Protection Program management work with ECC management to update CAL FIRE's procedures handbooks to reflect current practices in the field that differ from documented policies and procedures.

Anthony P. Favro

Anthony P. Favro, Chief
Office of Program Accountability

August 16, 2010

Findings and Recommendations

Finding #1 – Server Rooms Inadequately Secured

Condition:

The locking mechanism on the server room door is either missing or not used in six of the 13 units observed in the field. Additionally, one unit that was not visited indicated on its survey response that the ECC server room is not locked.

Another ECC server room remains locked at all times; however, the key that opens the lock is the same key for all offices throughout the building. Any employee with a key to an office for that building can access the server room. The ECC Chief stated that a combination lock will be installed to secure the room.

An eighth ECC server room remains unlocked; however, the floor captain must get permission from the ECC Chief to enter the server room.

Criteria:

Section 8114 of the *Command and Control Handbook (8100)* states that as the hub of CAL FIRE's communications system, the command and control centers elicit a great deal of interest from the public, the media, and CAL FIRE's own employees. To operate efficiently, each facility must accommodate the needs of command center personnel and prevent access by persons not directly involved in command center operations.

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of financial institutions. The FFIEC states that telecommunications closets should be locked.

TechRepublic is a website that helps IT decision-makers identify technologies and strategies to empower workers and streamline business processes. The site delivers a unique blend of original content by IT professional, peer-to-peer advice from the largest community of IT leaders on the Web, and a vast library of professional resources from the leading vendors in the IT industry. TechRepublic features blogs, community forums, vendor white papers, software downloads, Webcasts, and research. TechRepublic states that the number one most essential security measure that should be implemented is to lock up the server room, and that policies should set out who has the key or key code to get in.

Cause:

The server rooms are housed within the ECCs, which have physical access controlled; however, in general, ECC personnel rely on perimeter and building security to grant only authorized personnel access to the ECCs and server rooms, even during incidents when access controls tend to be more relaxed.

Effect:

If server rooms are not properly secured, the opportunity exists for non-authorized personnel to enter areas where crucial ECC equipment is maintained. The server room is the heart of the physical network, and someone with physical access to the servers, switches, routers, cables, and other devices in that room can do enormous damage.

Recommendation:

Ensure that ECC server room doors are locked at all times and that access is restricted to only authorized individuals. Install locks on server room doors that do not have one. Consider using a combination lock to provide a unique locking mechanism.

Response:

Headquarters IT, in conjunction with the Northern Region (CNR) and Southern Region (CSR) Command and Control personnel, shall identify which rooms require locked doors and who has authorized access to be in compliance with recommended server room security standards. CNR and CSR Technical Services Programs will coordinate installation of appropriate security hardware as budget and workload allow.

Anticipated Completion Date: May 1, 2011

Auditor Response:

OPA concurs with the auditee's response and will plan follow-up correspondence upon the proposed completion date.

Finding #2 – Inadequate Server Room Circulation

Condition:

Two of the 13 ECCs observed have inadequate server room circulation. One ECC server room utilizes three undersized air conditioners. On unusually hot days, the server room door is left open to help ventilate the room to keep equipment cool. Additionally, the outside door adjacent to the server room is left open to aid in circulation and the perimeter fencing is broken and remains open, which allows anyone off the street to walk in.

Another ECC server room is underserved by a small wall air conditioner. This air conditioning unit has in the past failed to provide sufficient cooling, resulting in the shut-down of all servers.

Criteria:

The Building Industry Consulting Service International (BICSI) is an organization whose certifications are considered the defacto certification for designers who specialize in complex voice/data cable layouts. There are standards for constructing server rooms and BICSI documents some of the best standards. Standards for server room environment control include:

- HVAC to provide constant temperature and humidity control in degrees C and the Relative Humidity (RH) based on the standards for active or passive components.
- Specify the minimum number of air changes per hour.
- Calculate the cooling in cubic meters per hour of 12 C cool air based on the number of 20 A circuits.
- Intake and exhaust of HVAC at 2.6m above finished floor (AFF).
- Need for a secondary cooling system and/or temperature alarm system. NOTE: Air conditioning systems will freeze in the winter if it is cold enough.

Cause:

The server room houses the Department's computer system servers, which release large amounts of heat.

Effect:

If the servers overheat, they will shut down and terminate all communications. The servers must then cool down before they will restart. This has occurred at least twice in the previous 12 months at one ECC.

Recommendation:

Ensure that server room temperatures are kept at a level that will allow for sufficient cooling of vital communication devices. Increase the air-conditioning in server rooms to adequately cool the equipment. Eliminate the need to leave doors open that will unnecessarily expose server room equipment and prevent overheating that will lead to shut down.

Response:

Typically, programmatic driven increases have exceeded the initial design criteria for equipment and associated heat loads utilized. HQ IT and Sacramento and Region Technical Services will survey the equipment in all of the ECCs. Sacramento Technical Services will provide designs to resolve the HVAC issues identified.

Region Technical Services will implement the required upgrades and/or repairs as top priority special repair projects.

The survey will be completed by March 2011; repair timelines will be contingent on available funding.

Auditor Response:

OPA concurs with the auditee's response and will plan follow-up correspondence upon the proposed completion date. Additionally, OPA recognizes that this mitigation effort is contingent upon individual ECC budgets, and, as such, mitigation plans may extend beyond the March 2011 date.

Finding #3 – Active Sprinkler Systems

Condition:

Server rooms have active sprinkler systems in two of the 13 ECCs visited. At the beginning of this audit, OPA had not included fire suppression in the audit plan. However, as the audit progressed, auditors observed that active water sprinkler systems were in use in at least two ECCs.

Criteria:

The mission of the international, nonprofit National Fire Protection Association (NFPA), established in 1896, is to reduce the worldwide burden of fire and other hazards on the quality of life by providing and advocating consensus codes and standards, research, training, and education. The world's leading advocate of fire prevention and an authoritative source on public safety, NFPA develops, publishes, and disseminates more than 300 consensus codes and standards intended to minimize the possibility and effects of fire and other risks. NFPA membership totals over 75,000 individuals and organizations around the world, including CAL FIRE.

NFPA 76, Fire Protection of Telecommunications Facilities, is a standard that provides requirements for fire protection of telecommunications facilities where telecommunications services, such as telephone (landline, wireless) transmission, data transmission, internet transmission, voice-over internet protocol (VoIP) transmission, and video transmission are rendered to the public.

Section 8.6.2.1.1 of *NFPA 76* states:

> Automatic fire suppression systems provided in telecommunications facilities should be selected with due consideration given to the hazards being protected and the impact of the agent on energized equipment. Facilities should be protected from accidental discharge of extinguishing agents to prevent damage to equipment or danger to personnel.

Section 8.6.2.1.2 of *NFPA 76* states:

> Fire suppression agents should not cause severe damage to the equipment. Suppression agents such as those containing dry chemical agents or corrosive wet agents in fixed systems should not be used in any area containing telecommunications equipment.

Cause:

Server rooms are often designed around what is available to IT staff when moving into a new location. Often a building must be retrofitted to accommodate such a resource.

If sprinklers are installed in the building, the sprinklers in the server room are rarely disconnected or mitigated by use of separating controls. The sprinkler systems use water and remain "charged" in the event of a fire.

Effect:

If a sprinkler system that uses water is discharged in an environment that is heavy in the use of electricity, damage will likely be more destructive. Servers and other IT resources in use in the server room require large amounts of electricity to operate. Water sprinklers discharging in an electrical environment could cause more damage than mitigated. Additionally, live electrical appliances in a wet environment could pose a threat to fire fighting staff.

Recommendation:

Immediately terminate water supply to server rooms and update with approved method. At minimum, require temperature sensors in water sprinklers to be set above alternate fire suppression methods. Work towards compliance with *NFPA 76*, Chapter 8. Notify ITS management of the standard for future planning purposes.

Response:

Sacramento and Region Technical Services will survey concurrently with the other surveys in Findings 1-5 all of the ECCs and determine which CAL FIRE ECCs require fire protection system modifications.

Sacramento Technical Services will provide the applicable designs to bring the ECCs fire protection systems up to current codes and standards.

Region Technical Services will implement the designs as top priority special repair projects.

The survey will be completed by March 2011; repair timelines will be contingent on available funding.

Auditor Response:

OPA concurs with the auditee's response and will plan follow-up correspondence upon proposed completion date. Additionally, OPA recognizes that this mitigation effort is contingent upon individual ECC budgets, and, as such, that mitigation plans may exceed the March 2011 date. OPA also recognizes that server rooms were not part of original design in most ECCs and that server rooms were placed wherever possible. As such, planning and mitigation will have a significant economic impact on ECC budgets, and OPA recognizes that individual units may have to also work with ITS to implement repairs or changes.

Finding #4 – Lack of Temperature Alarm Sensor

Condition:

A temperature alarm system was not present in the server rooms of four of the 13 ECCs visited. A temperature alarm system provides an early warning system prior to an overheating condition.

Criteria:

The Building Industry Consulting Service International (BICSI) is an organization whose certifications are considered the defacto certification for designers who specialize in complex voice/data cable layouts. BICSI documents some of the best standards for constructing server rooms. Standards for server room environment control include the need for a secondary cooling system and/or a temperature alarm system.

Cause:

At one ECC, personnel believe that a temperature alarm is not needed because an individual walks into the server room every day to change data tapes and that person should be able to detect a change in temperature.

At another ECC, personnel stated that the activation of exhaust fans was their indicator that the server room temperature had increased.

OPA does not consider either of these procedures to be sufficient mitigation.

Two other ECCs did not identify mitigation procedures for elevated server room temperatures.

Effect:

If the servers overheat, they will shut down and terminate all communications. The servers must then cool down before they will restart. ECC operations will be interrupted as a result.

Recommendation:

Install temperature alarm systems in all server rooms that do not have one.

Response:

Region Technical Services will survey all of their respective ECCs and engage Sacramento Technical Services for designs to assure that all CAL FIRE ECC server rooms are equipped with temperature alarms.

Region Technical Services will implement the required upgrades and/or repairs as top priority special repair projects.

The survey will be completed by March 2011; repair timelines will be dependant on available funding.

Auditor Response:

OPA concurs with the auditee's response and will plan follow-up correspondence upon the proposed completion date. Additionally, OPA recognizes that this mitigation effort is contingent upon individual ECC budgets, and, as such, mitigation plans may exceed the March 2011 date.

Finding #5 – Crawlspace Access

Condition:

Access to a crawlspace at one expanded ECC is not secured, allowing uncontrolled access to communication lines.

Criteria:

Section 8114 of the *Command and Control Handbook (8100)* states that as the hub of CAL FIRE's communications system, the command and control centers elicit a great deal of interest from the public, the media, and CAL FIRE's own employees. To operate efficiently, each facility must accommodate the needs of command center personnel and prevent access by persons not directly involved in command center operations.

Cause:

The building that is used for the expanded ECC sits next to the ECC. On the North side of the expanded ECC is an entry crawlspace that is unsecured.

Effect:

An unauthorized individual could gain access and cause severe damage to sensitive CAL FIRE assets.

Recommendation:

Restrict all access to ECCs and expanded ECCs to authorized employees only. Add appropriate locking mechanisms to all access points that are not secured in order to restrict access.

Response:

CSR and CNR Technical Services Programs will survey their respective Unit ECCs to determine which ones are out of compliance with crawl space security measures and then coordinate installation of appropriate hardware as budget and workload allow.

Anticipated Completion Date: May 1, 2011

Auditor Response:

OPA concurs with the auditee's response and will plan follow-up correspondence upon the proposed completion date.

Finding #6 – Command Center Access

Condition:

It was noted in one ECC interview that during incidents the ECC occasionally became overcrowded with higher ranking employees who were not necessarily directly involved in the incident.

Criteria:

Section 8114 of the *Command and Control Handbook (8100)* states that as the hub of CAL FIRE's communications system, the command and control centers elicit a great deal of interest from the public, the media, and CAL FIRE's own employees. To operate efficiently, each facility must accommodate the needs of command center personnel and prevent access by persons not directly involved in command center operations.

Cause:

It is common for CAL FIRE staff to want to assist in difficult times; however too many staff in an ECC during an incident can interrupt communications, cause confusion, lead to differing directives, and generally inhibit the ECC staff's ability to perform its jobs.

Effect:

Staff of ECC can receive conflicting orders and directives and be distracted.

Recommendation:

Allow only those individuals that the ECC Duty Chief deems necessary into the ECC. Ensure that all unit staff, regardless of rank, respect the authority granted to the ECC Duty Chief and adhere to policy and procedures.

Response:

CNR and CSR Region Chiefs will write a memo to their respective Unit Chiefs directing them to review section 8114 of the 8100 handbook to assure that their ECC command floor operations are insulated from unnecessary distractions from non-essential personnel.

Anticipated Completion Date: November 1, 2010

Auditor Response:

OPA concurs with the auditee's response and will plan follow-up correspondence upon the proposed completion date.

Finding #7 – Expanded Command Center Access

Condition:

Operations at one expanded command center ECC are easily interrupted during an expanded ECC incident, due to lack of controlled access to the area being used for the expanded operations.

Criteria:

Section 8114 of the *Command and Control Handbook (8100)* states that as the hub of CAL FIRE's communications system, the command and control centers elicit a great deal of interest from the public, the media, and CAL FIRE's own employees. To operate efficiently, each facility must accommodate the needs of command center personnel and prevent access by persons not directly involved in command center operations.

Cause:

The room used for the expanded ECC is a conference room in an adjoining building. This room has two entrances, one of which is the back door for the entire building. As such, traffic is very high through this area. When an incident requiring an expanded ECC occurs, control over access becomes even more difficult.

Effect:

The ease of egress in the expanded ECC can cause loss of clear communication, loss of direction, unauthorized persons in area, and can lead to lack of focus as ECC employees can be distracted.

Recommendation:

Take appropriate steps to ensure that access to all expanded ECCs is controlled.. Where necessary, identify alternate locations for expanded ECCs that can be properly secured to control physical access.

Response:

CNR and CSR Operations and Technical Services staffs will survey their respective units' primary expanded dispatch facilities and make both policy and infrastructure recommendations to assure access control and expanded dispatch facility reliability. These recommendations will be considered for current and future expanded dispatch facility planning and policy amendment.

Anticipated Completion Date: September 2011

Auditor Response:

OPA concurs with the auditee's response and will plan follow-up correspondence upon the proposed completion date.

Finding #8 – Disaster Recovery Plan Location

Condition:

Three of the ECCs visited has not identified a location to which to relocate if required by a major disaster.

Criteria:

SAM Section 5355.1 (Disaster Recovery Planning) defines disaster recovery planning and requires each agency to participate in disaster recovery planning processes to reduce the risks associated unanticipated outages for their critical applications and systems. Section 5355.1 also states that recovery strategies must be developed and updated routinely to anticipate risks including loss of utility (hardware, software, power, telecommunications, etc.), loss of access to the facility, and loss of facility.

Additionally, SAM Section 5355.2 (Agency Disaster Recovery Plan) requires each agency to maintain a Disaster Recovery Plan (DRP) that identifies the computer applications that are critical to agency operations, the information assets that are necessary for those applications, and the agency's plans for resuming operations following an unplanned disruption of those applications. This section also states that DRPs should be kept up-to-date.

The California Office of Information Security (OIS) is the primary state government authority in ensuring the confidentiality, integrity, and availability of state systems and applications, and ensuring the protection of state information. In accordance with SAM Sections 5355.1 and 5355.2, OIS has developed SIMM 65A, *Disaster Recovery Plan Documentation for Agencies Instructions,* which describes the minimum requirements for DRP development.

Section 1.0 of the SIMM 65A is entitled "Minimum DRP Requirements." Within Section 1.0, several subsections address relocation:

- Subsection 3.0, Recovery Strategy, states that a DRP should be built to accommodate a worst case scenario, i.e., the loss of service and the facility, and should include consideration of whether the agency's information technology infrastructure will be rebuilt at another location. In addition, this item states that the DPR should detail alternate recovery sites, including location, contact numbers, and the type of facilities/equipment that will be available.

- Subsection 5.0, Disaster Recovery Procedures, states that a DRP should include the process for recovering the critical data-processing activities, application and data recovery, and the process for suspending non-critical activities and any relocation to an interim (back-up) processing site.

- Subsection 7.0, Resource Requirements, states that a DRP should include a comprehensive list of the equipment, space, telecommunication needs, data, software, hard-copy references (forms and procedures), and personnel necessary for recovery, and it should document the resources that will be available at an alternate site.

Cause:

Three ECCs have not identified suitable locations for relocation and operational recovery in the event of major disaster.

Effect:

If these three current ECC locations were lost to disaster, the ECCs would not be able to relocate and begin operations, thus leaving the unit vulnerable and lacking communications and direction.

Recommendation:

Ensure that all ECCs have identified and documented adequate locations to which to relocate in the event of a major disaster that impacts the current locations. Maintain such locations as required.

Response:

CNR and CSR will survey the backup locations for each of their respective ECCs. For those units that do not have a backup, Fire Protection, CSR, and CNR will discuss the redeployment of current Mobile Communications Centers (MCC), and develop justification for additional MCCs to act as a catastrophic backup.

Anticipated Completion Date: July 2011

Auditor Response:

OPA concurs with the auditee's response and will plan follow-up correspondence upon the proposed completion date.

Finding #9 – Outdated Disaster Recovery Plan

Condition:

One of the 13 ECCs visited has a Disaster Recovery Plan that needs to be updated.

Criteria:

SAM Section 5355.1 (Disaster Recovery Planning) defines disaster recovery planning and requires each agency to participate in disaster recovery planning processes to reduce the risks associated unanticipated outages for their critical applications and systems. Section 5355.1 also states that recovery strategies must be developed and updated routinely to anticipate risks including loss of utility (hardware, software, power, telecommunications, etc.), loss of access to the facility, and loss of facility.

Additionally, SAM Section 5355.2 (Agency Disaster Recovery Plan) requires each agency to maintain a Disaster Recovery Plan (DRP) that identifies the computer applications that are critical to agency operations, the information assets that are necessary for those applications, and the agency's plans for resuming operations following an unplanned disruption of those applications. This section also states that DRPs should be kept up-to-date.

Cause:

The unit's current disaster recovery plan was developed in 1987. Although the current ECC Chief has added 3-4 pages of updates to primarily address electronic developments since the original plan was developed, there remain sections of the plan that have not been updated in more than 20 years.

Effect:

In the event of a major disaster, the ECC may be ill-prepared. Clear policy and procedures to be used in such an event do not exist.

Recommendation:

Ensure that all units have an up-to-date and comprehensive disaster recovery plan that is disseminated appropriately.

Response:

CNR and CSR Region Chiefs will write a memo to their respective Unit Chiefs directing them to update their disaster recovery plan and to assure training of critical personnel in plan contents and a continuous schedule of drills on plan elements.

Anticipated Completion Date: January 2011

Auditor Response:

OPA concurs with the auditee's response and will plan follow-up correspondence upon the proposed completion date.